

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Vialen, et al Serial No.: UNKNOWN
Filed: CONCURRENT HERewith Docket No.: 930.339USW1
Title: INTEGRITY CHECK IN A COMMUNICATION SYSTEM

CERTIFICATE UNDER 37 CFR 1.10

'Express Mail' mailing label number: EL887038794US

Date of Deposit: 10/10/01

I hereby certify that this correspondence is being deposited with the United States Postal Service 'Express Mail Post Office To Addressee' service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

By:

Name: Kari Arnold

PRELIMINARY AMENDMENT

Box Patent Application
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Please enter the following preliminary amendment into the above-referenced application.

CLAIMS

Please amend claims 6-7, 9-10, 13-15 and 17-18 as follows. A clean copy of the amended claims is included below. A marked up copy of the entire claim set is included in Appendix A.

1. A method of communication between a first node and a second node, a plurality of different channels being provided between said first and second node, said method comprising the steps of:
calculating an integrity output, said integrity output being calculated from a plurality of values, some of said values being the same for said different channels, at least one of

said values being arranged to comprise information relating to the identity of said channel, each channel having a different identity; and transmitting information relating to the integrity output from one of said nodes to the other.

2. A method as claimed in claim 1, wherein a separate input is provided for said information relating to the identity of the channel.
3. A method as claimed in claim 1, wherein said information relating to the identity of the channel is combined with at least one other input value.
4. A method as claimed in claim 3, wherein said information relating to the identity of the channel is combined with only one other input value.
5. A method as claimed in claim 3, wherein said combined input value input comprises a first part allocated to the identity of the bearer and a second part allocated to the other information provided by said value.
6. (AMENDED) A method as claimed in claim 1, wherein said values input to said algorithm comprise one or more of the following values:
an integrity key; a direction value, a fresh value, a message value and a count value.
7. (AMENDED) A method as claimed in claim 3, wherein said information relating to the identity of the bearer is combined with one or more of the following values input to said algorithm: a fresh value; a count value; an integrity key; a direction value and a message value.
8. A method as claimed in claim 7, wherein said message value is sent from one node to another without the channel identification information.

9. (AMENDED) A method as claimed in claim 1, wherein the output of the integrity algorithm is sent from one node to another.
10. (AMENDED) A method as claimed in claim 1, wherein communication between said first and second nodes is via a wireless connection.
11. A method as claimed in claim 10, wherein one of said first and second nodes is user equipment.
12. A method as claimed in claim 12, wherein said user equipment is a mobile station.
13. (AMENDED) A method as claimed in claim 10, wherein one of said first and second nodes is a radio network controller.
14. (AMENDED) A method as claimed in claim 10, wherein one of said first and second nodes is a node B.
15. (AMENDED) A method as claimed in claim 1, wherein said communication channels comprise a radio bearer.
16. A method as claimed in claim 15, wherein said radio bearer is a signalling radio bearer.
17. (AMENDED) A method as claimed in claim 1, wherein said input values are input to an algorithm for calculation said output.
18. (AMENDED) A method as claimed in claim 6, wherein the same integrity key is used for the different channels.

19. A method for carrying out an integrity check for an system comprising a first node and a second node, a plurality of communication channels being provided between said first node and said second node, said method comprising the step of calculating an integrity output using a plurality of values, some of said values being the same for said different channels, at least one of said values being arranged to comprise information relating to the identity of said channel, each channel having a different identity.

20. A method of communication between a first node and a second node, a plurality of different channels being provided between said first and second node, said method comprising the steps of:

calculating an integrity output using a plurality of values, one of said values being an integrity key, each of said channels having a different integrity key; and
transmitting information relating to the output of said integrity algorithms from one of said nodes to the other.

21. A method of communication between a first node and a second node, a plurality of different channels being provided between said first and second node, said method comprising:

triggering an authentication procedure; and

calculating a desired number of integrity parameters by the authentication procedure.

22. A node, said node for use in a system comprising a said node and a further node, a plurality of different channels being provided between said nodes, said node comprising means for calculating an integrity output, said integrity output being calculated from a plurality of values, some of said values being the same for said different channels, at least one of said values being arranged to comprise information relating to the identity of said channel, each channel having a different identity; and
means for transmitting information relating to the integrity output from said node to said further node.

23. A node, said node for use in a system comprising said node and a further node, a plurality of different channels being provided between said nodes, said node comprising means for calculating an integrity output, said integrity output being calculated from a plurality of values, some of said values being the same for said different channels, at least one of said values being arranged to comprise information relating to the identity of said channel, each channel having a different identity; and means for comparing information relating to the integrity output calculated by said node with a value calculated by the further node.

24. An algorithm for calculating an integrity output for use in a system comprising a node and a further node, a plurality of different channels being provided between said nodes, said algorithm comprising means for calculating an integrity output, said integrity output being calculated from a plurality of values, some of said values being the same for said different channels, at least one of said values being arranged to comprise information relating to the identity of said channel, each channel having a different identity.

REMARKS

The above preliminary amendment is made to remove multiple dependencies from claims 6-7, 9-10, 13-15, 17-18 and reformatted for U.S. standards.

Applicant respectfully requests that this preliminary amendment be entered into the record prior to calculation of the filing fee and prior to examination and consideration of the above-identified application.

If a telephone conference would be helpful in resolving any issues concerning this communication, please contact Applicant's attorney of record, Michael B. Lasky at 952-912-0523.

Altera Law Group, LLC
6500 City West Parkway – Suite 100
Minneapolis, MN 55344-7701
952-912-0527

By:

Michael B. Lasky
Reg. No. 29,555
MBL/blj

1992-1993		1993-1994		1994-1995		1995-1996		1996-1997		1997-1998		1998-1999		1999-2000		2000-2001		2001-2002		2002-2003		2003-2004		2004-2005		2005-2006		2006-2007		2007-2008		2008-2009		2009-2010		2010-2011		2011-2012		2012-2013		2013-2014		2014-2015		2015-2016		2016-2017		2017-2018		2018-2019		2019-2020		2020-2021		2021-2022		2022-2023		2023-2024		2024-2025		2025-2026		2026-2027		2027-2028		2028-2029		2029-2030		2030-2031		2031-2032		2032-2033		2033-2034		2034-2035		2035-2036		2036-2037		2037-2038		2038-2039		2039-2040		2040-2041		2041-2042		2042-2043		2043-2044		2044-2045		2045-2046		2046-2047		2047-2048		2048-2049		2049-2050		2050-2051		2051-2052		2052-2053		2053-2054		2054-2055		2055-2056		2056-2057		2057-2058		2058-2059		2059-2060		2060-2061		2061-2062		2062-2063		2063-2064		2064-2065		2065-2066		2066-2067		2067-2068		2068-2069		2069-2070		2070-2071		2071-2072		2072-2073		2073-2074		2074-2075		2075-2076		2076-2077		2077-2078		2078-2079		2079-2080		2080-2081		2081-2082		2082-2083		2083-2084		2084-2085		2085-2086		2086-2087		2087-2088		2088-2089		2089-2090		2090-2091		2091-2092		2092-2093		2093-2094		2094-2095		2095-2096		2096-2097		2097-2098		2098-2099		2099-2100		2100-2101		2101-2102		2102-2103		2103-2104		2104-2105		2105-2106		2106-2107		2107-2108		2108-2109		2109-2110		2110-2111		2111-2112		2112-2113		2113-2114		2114-2115		2115-2116		2116-2117		2117-2118		2118-2119		2119-2120		2120-2121		2121-2122		2122-2123		2123-2124		2124-2125		2125-2126		2126-2127		2127-2128		2128-2129		2129-2130		2130-2131		2131-2132		2132-2133		2133-2134		2134-2135		2135-2136		2136-2137		2137-2138		2138-2139		2139-2140		2140-2141		2141-2142		2142-2143		2143-2144		2144-2145		2145-2146		2146-2147		2147-2148		2148-2149		2149-2150		2150-2151		2151-2152		2152-2153		2153-2154		2154-2155		2155-2156		2156-2157		2157-2158		2158-2159		2159-2160		2160-2161		2161-2162		2162-2163		2163-2164		2164-2165		2165-2166		2166-2167		2167-2168		2168-2169		2169-2170		2170-2171		2171-2172		2172-2173		2173-2174		2174-2175		2175-2176		2176-2177		2177-2178		2178-2179		2179-2180		2180-2181		2181-2182		2182-2183		2183-2184		2184-2185		2185-2186		2186-2187		2187-2188		2188-2189		2189-2190		2190-2191		2191-2192		2192-2193		2193-2194		2194-2195		2195-2196		2196-2197		2197-2198		2198-2199		2199-2200		2200-2201		2201-2202		2202-2203		2203-2204		2204-2205		2205-2206		2206-2207		2207-2208		2208-2209		2209-2210		2210-2211		2211-2212		2212-2213		2213-2214		2214-2215		2215-2216		2216-2217		2217-2218		2218-2219	
-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--	-----------	--

[illegible]

1. A method of communication between a first node and a second node, a plurality of different channels being provided between said first and second node, said method comprising the steps of:
calculating an integrity output, said integrity output being calculated from a plurality of values, some of said values being the same for said different channels, at least one of said values being arranged to comprise information relating to the identity of said channel, each channel having a different identity; and
transmitting information relating to the integrity output from one of said nodes to the other.
2. A method as claimed in claim 1, wherein a separate input is provided for said information relating to the identity of the channel.
3. A method as claimed in claim 1, wherein said information relating to the identity of the channel is combined with at least one other input value.
4. A method as claimed in claim 3, wherein said information relating to the identity of the channel is combined with only one other input value.
5. A method as claimed in claim 3, wherein said combined input value input comprises a first part allocated to the identity of the bearer and a second part allocated to the other information provided by said value.
6. (AMENDED) A method as claimed in [any preceding] claim 1, wherein said values input to said algorithm comprise one or more of the following values: an integrity key; a direction value, a fresh value, a message value and a count value.
7. (AMENDED) A method as claimed in claim 3 [or 5 and 6], wherein said information relating to the identity of the bearer is combined with one or more of the following values input to said algorithm: [said] a fresh value; [said] a count value; an [said] integrity key; [said] a direction value and [said] a message value.
8. A method as claimed in claim 7, wherein said message value is sent from one node to another without the channel identification information.
9. (AMENDED) A method as claimed in [any preceding] claim 1, wherein the output of the integrity algorithm is sent from one node to another.
10. (AMENDED) A method as claimed in [any preceding] claim 1, wherein communication between said first and second nodes is via a wireless connection.

11. A method as claimed in claim 10, wherein one of said first and second nodes is user equipment.
12. A method as claimed in claim 12, wherein said user equipment is a mobile station.
13. (AMENDED) A method as claimed in [any of] claim[s] 10 [to 12], wherein one of said first and second nodes is a radio network controller.
14. (AMENDED) A method as claimed in claim 10, [11, 12 or 13,] wherein one of said first and second nodes is a node B.
15. (AMENDED) A method as claimed in [any preceding] claim 1, wherein said communication channels comprise a radio bearer.
16. A method as claimed in claim 15, wherein said radio bearer is a signaling radio bearer.
17. (AMENDED) A method as claimed in [any preceding] claim 1, wherein said input values are input to an algorithm for calculation said output.
18. (AMENDED) A method as claimed in claim 6 [or any claim appended thereto], wherein the same integrity key is used for the different channels.
19. A method for carrying out an integrity check for an system comprising a first node and a second node, a plurality of communication channels being provided between said first node and said second node, said method comprising the step of calculating an integrity output using a plurality of values, some of said values being the same for said different channels, at least one of said values being arranged to comprise information relating to the identity of said channel, each channel having a different identity.
20. A method of communication between a first node and a second node, a plurality of different channels being provided between said first and second node, said method comprising the steps of:
calculating an integrity output using a plurality of values, one of said values being an integrity key, each of said channels having a different integrity key; and
transmitting information relating to the output of said integrity algorithms from one of said nodes to the other.
21. A method of communication between a first node and a second node, a plurality of different channels being provided between said first and second node, said method comprising:
triggering an authentication procedure; and
calculating a desired number of integrity parameters by the authentication procedure.

22. A node, said node for use in a system comprising a said node and a further node, a plurality of different channels being provided between said nodes, said node comprising means for calculating an integrity output, said integrity output being calculated from a plurality of values, some of said values being the same for said different channels, at least one of said values being arranged to comprise information relating to the identity of said channel, each channel having a different identity; and means for transmitting information relating to the integrity output from said node to said further node.

23. A node, said node for use in a system comprising said node and a further node, a plurality of different channels being provided between said nodes, said node comprising means for calculating an integrity output, said integrity output being calculated from a plurality of values, some of said values being the same for said different channels, at least one of said values being arranged to comprise information relating to the identity of said channel, each channel having a different identity; and means for comparing information relating to the integrity output calculated by said node with a value calculated by the further node.

24. An algorithm for calculating an integrity output for use in a system comprising a node and a further node, a plurality of different channels being provided between said nodes, said algorithm comprising means for calculating an integrity output, said integrity output being calculated from a plurality of values, some of said values being the same for said different channels, at least one of said values being arranged to comprise information relating to the identity of said channel, each channel having a different identity.